Big Brother's little, more dangerous brother

Mark Klamberg 2021-06-01T10:23:12

The European Court of Human Rights (ECtHR) issued on 25th May 2021 judgments in two connected cases: *Big Brother Watch v. UK* and *Centrum för Rättvisa v. Sweden*. Both cases involved the review of bulk interception of communications, described by its critics as "mass surveillance", or in the industry concerned as "signals intelligence". The judgments have by some been described as a win for privacy, while others are more pessimistic, portraying them as the "grand normalization of mass surveillance". I find the later view more accurate. This post will examine the *Centrum för Rättvisa v. Sweden* case (hereafter: *Centrum för Rättvisa*) by examining the Swedish signals intelligence act and associated legislation as implemented by the Swedish equivalent to the NSA; BND and GCHQ: Försvarets Radioanstalt (FRA, in English: National Defence Radio Establishment,).

The FRA may, pursuant to the Signals Intelligence Act, conduct surveillance vis-a-vis communications crossing Swedish borders to survey eight phenomena (2008:717, Section 1(2)), including external military threats to the country, strategic circumstances concerning international terrorism or other serious cross-border crime and foreign intelligence operations against Swedish interests.

The Swedish example is interesting, since it has attracted less criticism from the ECtHR compared to the UK, and as such may be portrayed as a model law for those actors in favour of this type of surveillance. However, the Swedish legislation is highly opaque. The ECtHR has fallen short in neither scrutinizing any of the case law from the Swedish Foreign Intelligence Court (Försvarsunderrättelsedomstolen), nor any of the FRA's actual practice.

Leaks, Public Debate and the Legalization of Bulk Interception of Communications

The *Centrum för Rättvisa* case was filed in 2008 in the context of a public debate in Sweden on the adoption of the Swedish Signals Intelligence Act and other associated statutes (collectively referred to as the "FRA law"). During this debate, the Swedish Public service broadcaster (SVT) published secret documents from a leak within FRA. This leak contradicted how the Government and FRA described the scope and nature of the Swedish signals intelligence operations. Thus, Sweden already had its domestic equivalent of the Snowden revelations and public debate in 2007-2008. The NGO *Centrum för Rättvisa* made two interventions of particular relevance to this debate: First, they suggested introducing a 9-point programme on how the legislation should be amended, while still allowing the FRA to conduct signals intelligence operations. Second, *Centrum för Rättvisa* filed a complaint to

the ECtHR which concerned three time periods: 1) previous operations of the FRA (when there was no law explicitly permitting signals intelligence), 2) the legislation adopted June 2008 and 3) the legislation to be amended 2009 following a political agreement in September 2008. Thus, the aim of *Centrum för Rättvisa* was not to prohibit signals intelligence operation against civil communications, instead it was to improve how it was regulated. It is also in this context we should view the judgment by the ECtHR.

Sweden was not the first European country to have this debate or to have their system under review by the ECtHR, as illustrated by the two cases *Weber and Saravia v. Germany* and *Liberty v. UK*. *Centrum för Rättvisa* relied on both these cases in their op-ed and complaint to the ECtHR. Thus, there was debate on surveillance several years before the Snowden revelations. The similar timing in several European countries may be explained with four major changes during the 1990s: 1) technological development towards fibre optic cable, 2) expanding perceptions of national security and threats thereto, 3) increased demands to be compliant with human rights law and 4) the privatisation of previously state-owned communication providers. These changes created a need to reform both the tools of electronic surveillance and domestic legislation. Surveillance that was previously kept secret became subject to public debate and scrutiny.

The Centrum för Rättvisa case

Turning to the Swedish legislation on signals intelligence and the *Centrum för Rättvisa* case. The 2008 act created a legal obligation for communication providers to transfer all communications crossing Swedish borders to certain “collection points”, which may include communication where the sender or receiver is in Sweden (The Electronic Communications Act 2003:389, chapter 6, section 19(a); Government Bill 2006/07:63, p. 83). The legislation provides safeguards in the form of: limited access for the FRA to certain “communication carriers” (signalbärare) (Signals Intelligence Act, sections 4 a § p.2 and 5 a § p.2), eight specified purposes for which communications may be collected (Signals Intelligence Act, sections 1 § 2), collection requires prior approval by the Defence Intelligence Court (Signals Intelligence Act, 4 a §, 5 § and 6 § and Act (2009:966) on the Defence Intelligence Court) and ex post facto review by the Foreign Intelligence Inspectorate (Statens inspektion för försvarsunderrättelseverksamheten; Foreign Intelligence Inspectorate Instructions Ordinance, SFS 2009:969).

All of this may look like adequate protection for privacy. It persuaded the first Chamber which reviewed the case, and almost entirely also the Grand Chamber. On 19 June 2018, a Chamber of the ECtHR unanimously held that there had been no violation of Article 8 of the Convention and that there was no need to separately examine the complaint under Article 13. After referral, the Grand Chamber issued its judgment on 25 May 2021. Several aspects are worth noting. The Grand Chamber addressed jointly the “in accordance with the law” and “necessity” requirements (§ 248). To justify why there was a need to develop the case law, the Grand Chamber explained that in *Weber and Saravia* and *Liberty*, the Court did not expressly address the fact that it was dealing with surveillance of a different nature and scale

from that considered in previous cases (§ 256). In the context of bulk interception and retention of communications data, such data should be analysed by reference to the same safeguards as those applicable to content (§ 277). The Grand Chamber found that Sweden had been in violation of Article 8 based on three points: 1) the absence of a clear rule on destroying intercepted material which does not contain personal data; 2) the absence of a requirement in the Signals Intelligence Act or other relevant legislation that, when making a decision to transmit intelligence material to foreign partners, consideration is given to the privacy interests of individuals; and 3) the absence of an effective *ex post facto* review (§§ 369-377).

What the Court fails to discuss

Arguably, the three concerns of the Grand Chamber are solvable. As such, one could portray the Swedish legislation as a model, possible for other countries to emulate. However, there are some remaining fundamental problems, which the safeguards listed above don't address and that the majority of the Court fails to discuss. A communication carrier is described in the law and its preparatory works (which is a source of law in Sweden) as a fibre-optic core (Government Bill 2008/09:201, p. 36). When I and fellow experts from other fields reviewed this matter in 2009, taking into account data provided by the FRA, one fibre-optic core could carry 400 Gigabit/s (Parliamentary committee on defence affairs, 2007/08:FöU14, pp. 76-77), the equivalent of 200 000 internet users' communications at the time, expected to increase to 1 600 000 users by 2011, as a result of technological improvement on fibre-communications. There is no limit in the law on how many signal carriers/fibre optic cores the FRA can access – it is based on what the FRA "needs" (Signals Intelligence Act, sections 4 a § p.2), without any further specification in the law. When getting access to additional signal carriers/fibre optic cores, there is no requirement to make a proportionality assessment in relation to the total number the FRA already has access to.

The eight specified purposes for which FRA can conduct surveillance are supplemented in the law by an additional purpose described as "development activities" to monitor the "ever-changing signals environment, technical developments and signals protection" (Signals Intelligence Act, section 1(3)). There are several indications that the development activities involve the collection and retention of large amounts of metadata. The Swedish Government argues that this is somehow separate from the narrower "intelligence activities". However, the FRA is authorized to transfer data collected for the purpose of "development activities" to "intelligence activities" (Government Bill 2006/07:46, p. 68). Judge Pinto accurately describes this as a "true legal black hole" (Concurring Opinion § 7).

Moreover, the prior approval of the Defence Intelligence Court should not be confused with an individualized court warrant for wiretap or access to certain records. The Defence Intelligence Court approves a selector (sökbegrepp) or categories of selectors that will be utilized during collection (Signal Intelligence Act, section 4(a)). A selector is typically not related to a specific person (Signal Intelligence Act, section 3(2) and 5(5); Government Bill 2008/09:201, pp. 24, 44, 46, 53). Lastly, as noted by the Grand Chamber, the Foreign Intelligence

Inspectorate has a dual role in taking or authorising operational decisions such as those concerning access to the communication carriers and *ex post facto review* on request from individuals, which may create a conflict of interests (§ 359, § 364).

In sum, the Swedish legislation on bulk interception of communication contains a lot of rules and provides for a Defence Intelligence Court which may give the impression that it is well regulated and supervised. However, the existence of legal rules and institutions does not necessarily mean that a potentially harmful practice is restrained – law may also operate as enabling these practices. In order to make a proper assessment of Sweden's bulk interception of communications, the ECtHR should have examined the actual case law from the Intelligence Court and the practice of the FRA. Obviously, it would be impossible for the FRA to reveal the concrete intelligence targets of its surveillance and penetrated codes. However, if the FRA's capabilities are used in matters traditionally in the law enforcement domain, such as terrorism and cross-border crime, greater transparency and scrutiny is needed.

A final question is raised by the joint declaration of the Judges Kjølbro and Wennerström. They both voted to find no violation of Article 8 of the Convention. They made a reference in one sentence to the reasoning of the chamber (the judgment of 19 June 2018), and added only that they would "refrain from elaborating on our legal arguments in this case and limit [themselves] to this declaration of vote". In the absence of legal arguments, what was determinative for these two judges? Moreover, as noted by Judge Pinto, the majority appear to assume the veracity of the Government's pleadings without really putting them to the test. The lack of proper scrutiny may be explained in several ways, including the potential absence of technological knowledge and perception that national security is ultimately a matter for the executive and not the courts. This begs the question whether courts – domestic and international – will ever be in a position to exercise effective control when states are conducting surveillance for national security reasons.
